

Standardising a Moving Target: The Development and Evolution of IoT Security Standards

Irina Brass Leonie Tanczer Madeline Carr Miles Elsdén Jason Blackstock

*Dept. of Science, Technology, Engineering & Public Policy
University College London, 36–38 Fitzroy Square, London, W1T 6EY, UK
{i.brass, l.tanczer, m.carr, m.elsden, jason.blackstock}@ucl.ac.uk*

Keywords: IoT security standards, certification, compliance.

Abstract

The standards landscape for IoT security is currently developing in a fragmented manner. This paper provides a review of the main IoT security standards and guidelines that have been developed by formal standardisation organisations and transnational industry associations and interest alliances to date. The review makes three main contributions to the study of current IoT standards-development processes. First, governments and regulatory agencies in the EU and the US are increasingly considering the promotion of baseline IoT security requirements, achieved through public procurement obligations and cybersecurity certification schemes. Second, the analysis reveals that the IoT security standards landscape is dominated by de facto standards initiated by a diverse range of industry associations across the IoT ecosystem. Third, the paper identifies a number of key challenges for IoT security standardisation, most notably: a) the difficulty of setting a baseline for IoT security across all IoT applications and domains; and b) the difficulty of monitoring the adoption, implementation and effectiveness of IoT security standards and best practices. The paper consequently contributes to a better understanding of the evolution of IoT security standards and proposes a more coherent standards development and deployment approach.

1 Introduction

The Internet of Things (IoT) is receiving increasing attention from industry, policy makers, consumers and the media. A recent report commissioned by OFCOM – the communications regulator in the UK – estimated that the number of IoT connections in the UK will reach 155.7 million by the end of 2024, at an expected compound average growth rate of approximately 36% [1]. This growth can be explained by a number of factors, including the increased adoption of IoT consumer products, especially in the EU, the US and South-East Asia [2], as well as by the “business transformation” that IoT promises in terms of increased efficiency and revenue, risk management and costs reduction [3].

However, increased device connectivity and process integration have exposed new vulnerabilities in IoT device security, data integrity and system reliability. In 2016, compromised IoT devices located all over the world were used to produce the most powerful DDoS attack ever recorded against a DSN, at 1-TBps. This led security analysts at Cisco to conclude that security weaknesses in IoT devices and systems have brought about new attack strategies, coined as “Destruction of Service” (DeOS) [4]. IoT security is thus becoming central to businesses and the public sector. In 2017, Ovum found that “data security and privacy concerns”, “legacy IT infrastructure and systems” and “the lack of a robust business case” were reported as the top three barriers to the deployment of IoT [5].

IoT security standards, especially common and open standards, play a crucial role in lowering these barriers to acceptability, adoption and deployment of the IoT [6–8]. A recent survey conducted by the PETRAS IoT Research Hub, BSI and IoTUK showed (Figure 1) that public and private organisations use IoT cybersecurity standards for several reasons, most notably

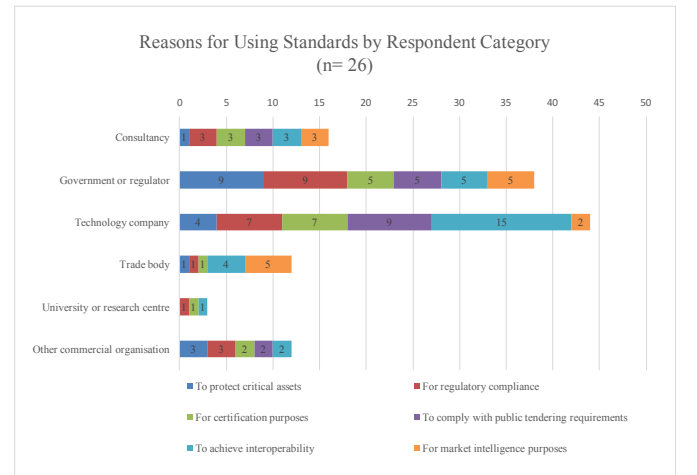


Fig. 1: Reasons for Using Standards Related to Cybersecurity of the IoT. Data shows responses to Question 9 of the ‘Cybersecurity of the Internet of Things Standards Survey’ [9]: “Please tell us what goal the standards you identified support. Select all that apply.”

to achieve interoperability (22.9%), for regulatory compliance (18.3%), for certification purposes (14.5%) and for compliance with public tendering (14.5%) [9].

Policy makers, regulatory agencies and the industry are also increasingly agreeing that a *baseline for IoT security* is required to ensure data protection, service continuity and public safety [10–13]. Yet, given the diversity of IoT application areas and domains, *what this security baseline should include and how it should be implemented and monitored*, is still a matter for debate.

1.1 Scope of the Paper

This paper provides a review of the main trends in the development and evolution of IoT security standards to date. It aims to offer a detailed analysis of the extent to which standardisation efforts are leading towards the *establishment of a baseline for IoT security* in some of the most developed IoT markets [2], with particular focus on the UK, EU and US. Standards are defined here broadly to include principles, guidelines, codes of practice and technical specifications that are developed by public, private and not-for-profit entities, including government departments and agencies, national standardisation bodies, industry alliances and associations¹.

Although the paper makes reference to some of the key IoT security standards for specific domains, such as connected autonomous vehicles, medical devices and industrial applications, it does not provide a comprehensive review of standards for each IoT application area. Instead, it focuses on what industry and the public sector have currently identified as technical and organisational specifications for default IoT security.

1.2 Methodology

This paper summarises findings of an ongoing study conducted by the Standards, Governance and Policy (SGP) team of the PETRAS IoT Research Hub, which examines *the dynamics between voluntary standards and mandatory regulatory frameworks* for ensuring the adoption of a baseline of IoT security.

The research is underpinned by methodological triangulation based upon:

1. Desk-based research of IoT security guidelines, codes of practice and technical specifications, developed by public, private and not-for-profit organisations;
2. An online ‘Cybersecurity of the Internet of Things Standards Survey’, exploring the use and implementation of

¹ This broad definition is adopted because technical (or design) specifications represent only one type of standards, which generally address behaviour at the *prevention stage*. As outlined in the specialist literature, standards can also focus on “the *act* that gives rise to a harmful result” – known as performance standards, such as risk assessment in the context of cybersecurity, or they can focus on “the *harmful result* itself” – known as target standards, such as joint incident responses conducted by CERTs. For a foundational description of standards typologies, see Baldwin et al [14].

IoT security standards, conducted by PETRAS IoT, BSI and IoTUK (March 2017);

3. A workshop on ‘IoT Security by Default’ with PETRAS IoT researchers and partners, exploring standards development in IoT consumer goods, transport, health, and utilities (March 2017).

A fourth stage, consisting of a series of semi-structured interviews with key standards development organisations, trade associations and UK regulatory bodies, is currently being conducted in order to gather more evidence on the barriers to the adoption and implementation of IoT security standards.

1.3 Key Findings

This paper puts forward the following findings, as discussed in the sections below:

1. While the policy and regulatory status quo is still based on a ‘light touch’ approach to standardising IoT security, governments and regulatory agencies in the EU and the US are increasingly considering the promotion of baseline IoT security requirements, achieved through *public procurement obligations* and *cybersecurity certification schemes*.
2. This policy shift can be seen as a response to the slow pace of IoT security self-regulation achieved by the market. Specifically, the IoT security standards landscape is dominated by *de facto standards*, developed by a diverse range of industry alliances and associations across the IoT ecosystem. Although there is some *degree of convergence towards baseline specifications for IoT security* across these schemes, there is also considerable *competition between them*, evident in the parallel development of industry-led testing and certification schemes.
3. Two main gaps in the development of a commonly agreed baseline for IoT security can be identified. First, there is clear *divergence* across the reviewed standards *on the basic scope and relationship between IoT security, safety, consumer trust, trustworthiness and system integrity*. Second, at present, there is limited information about the *adoption, implementation and review rate of government and industry-led standards for IoT security*, which makes their effectiveness difficult to monitor and evaluate.

2 Policies, Regulatory Frameworks and High-Level Guidelines for IoT Security

The policy landscape for IoT security is currently mixed, especially across the three regions that are estimated to “represent 67% of the overall IoT installed base in 2017” – Western Europe, North America and East Asia [2]. Over the past years, governments and regulatory agencies across these regions have

promoted a ‘light touch’ approach to securing the IoT, issuing a combination of non-binding high level guidelines and sector-specific recommendations. In other words, governments have predominantly utilised their advisory and steering powers, rather than their rule-making capacity to promote IoT security.

In the UK, this approach was detailed in the ‘Cyber Security Regulation and Incentives Review’ conducted by HMG Department for Digital, Culture, Media and Sport (DCMS), which stated that “for now, [the UK] Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR” [15]. Simultaneously, the UK National Cyber Security Centre (NCSC) has developed a set of eight principles for ‘secure by default’ devices and systems, including security by design, transparency and usability [16].

This steering approach adopted by the UK Government does not mean that IoT data integrity and security are fully unregulated [17–19]. At present, several regulatory frameworks apply to aspects of IoT data integrity and security, such as the forthcoming General Data Protection Regulation (GDPR 2016/679) and the Network and Information Systems Directive (NIS 2016/1148). These require data protection impact assessments or cybersecurity risk assessments for organisations that use new technologies or provide essential services that result in a high risk to the rights and freedoms of individuals or the integrity of critical infrastructure. In addition, security guidelines for specific IoT applications have been put forward by other UK Government departments, such as the ‘Key Principles of Cyber Security for Connected and Automated Vehicles’ developed by HMG Department for Transport [20].

A similar policy landscape has taken shape in the US. In 2016, the US Department of Homeland Security produced a set of non-binding ‘Strategic Principles for Securing the IoT’, proposing an integrated, end-to-end approach to securing the IoT based on security by design as well as continuous product, system and business lifecycle risk assessment [21]. In addition, specialised agencies in the US have also promoted non-binding cybersecurity guidelines and recommendations for automated vehicles [22] and for medical devices [23], [24].

2.1 Mandating IoT Security?

Recently, the policy landscape for IoT security has undergone important changes that raise questions about the extent to which a *baseline for IoT security could be driven by new legislative and regulatory initiatives*. Two major developments are pointing in this direction: a) two legislative proposals in the US and the EU; and b) the increasing role of formal standardisation, communications and cybersecurity agencies in promoting detailed guidelines that apply to IoT security.

In August 2017, a bill entitled the ‘IoT Cybersecurity Improvement Act’ was introduced in the US Senate, proposing “minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for

other purposes” [25]. Currently in referral to the Committee on Homeland Security and Governmental Affairs, the proposed bill requires written proof of third-party security certification in public acquisition contracts and procurement of Internet-connected devices (Sec 3.1 A(i)).

In September 2017, the European Commission proposed a regulation that would formally establish the European Union Agency for Network and Information Security (ENISA) as the ‘Cybersecurity Agency’ of the EU. ENISA is tasked with several cybersecurity coordination and operational functions, including the preparation of an initially voluntary cybersecurity certification scheme based on three assurance levels (‘basic’, ‘substantial’, ‘high’) [26].

The proposed legislations make reference to key security principles and technical specifications which have been put forward by formal standardisation, communication and cybersecurity agencies in the US and the EU. These guidelines are increasingly converging towards a set of minimum specifications for IoT security at the device and at the system level (Figure 2).

At device level, minimum security requirements such as vulnerability disclosure, upgradability and service lifecycle management are proposed by a number of public agencies in the US, including the National Telecommunications and Information Administration (NTIA) [27] and the Federal Trade Commission (FTC) [28]. At the system level, authentication, authorisation, access controls, cryptographic key management as well as integrity management are proposed by the US National Institute of Standards and Technology (NIST) [29] and ENISA [30]. In addition, these agencies have set up several multistakeholder engagement processes for the continuous development and review of baseline requirements for security in IoT devices and critical infrastructure domains [11], [31–33].

Overall, the policy landscape in the UK, EU and US reveals increased convergence towards a baseline for IoT security. However, given that the proposed guidelines are supported by non-



High-Level Principles	Public Agencies	Implementation
Device Principles  - Vulnerability Disclosure - Upgradability - Patch Management... System Principles  - Encryption - Access Control - Integrity Management...	NTIA (2017) Multistakeholder Process; Internet of Things(IoT) Security Upgradability and Patching	US <i>Flexible</i> Certification Approach
	ENISA (2017) Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructure NIST (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	EU <i>Centralised</i> Certification Approach

Fig. 2: Converging Principles for IoT Security in Legislations and High-Level Guidelines (EU, US)

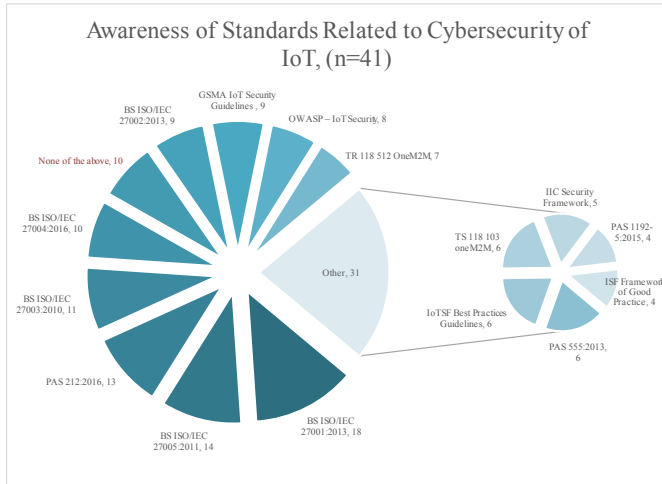


Fig. 3: Awareness of Standards Related to Cybersecurity of the IoT. Data shows responses to Question 3 of the ‘Cybersecurity of the Internet of Things Standards Survey’[9]: “Which of these standards have you heard of in relation to cybersecurity of the Internet of Things? Please select all that apply”.

binding frameworks and recommendations, it can be easily argued that a ‘light touch’ approach to IoT security continues to be the predominant policy option, at least at present.

While differences between the certification schemes in the US and the EU remain – with the US bill proposing a more flexible, contract-by-contract ‘written certification’ requirement (Sec 3.1 (i)), and the EU regulation proposing a more centralised scheme developed by ENISA (Art 44) – these developments could pave the way towards the emergence of an *international baseline for IoT security* [13].

3 Industry Codes of Practice, Technical Specifications and Certification Schemes

The recent policy shift towards the establishment of a baseline for IoT security via new legislation and certification can be, at least in part, explained by the *fragmented and increasingly competitive landscape for IoT security standardisation*.

The PETRAS IoT ‘Cybersecurity of the Internet of Things Standards Survey’ confirmed the fragmented standards landscape for IoT security [9]. When asked about their awareness of both *formal* and *de facto* standards² that apply to IoT cybersecurity, respondents showed limited convergence towards

² Formal standards, also known as *de jure* standards, are those developed and/or endorsed by formal standardisation organisations at domestic (e.g. BSI), regional (e.g. CEN/CENELEC) or international level (e.g. ISO). They are formal because they go through formalised adoption, review and audit processes. *De facto* standards, also known as market-driven standards, are developed either by single entities (e.g. companies) or by expert interest associations (e.g. GSMA, IoT Security Foundation). They are *de facto* because they become the predominant standard through market adoption.

a predominant standard (Figure 3). However, the ISO/IEC 27000 series of information security management standards emerged as most popular.

With regard to their awareness of *de facto* standards, the respondents identified the GSM Association (GSMA) IoT Security Guidelines [34–37] and the Open Web Application Security Project (OWASP) IoT Security Guidance [38–39] as the most well-known standards related to IoT security.

The distribution of responses in Figure 3 underlines pressing issues about IoT security standardisation. First, although relevant for IoT security, the ISO/IEC 27000 series of information security management standards does not apply to all components of the IoT ecosystem. There is, thus, a clear gap in the development of formal security standards specific to the IoT which take into account both device and end-to-end security. Second, formal standards development organisations (SDOs) have to clearly highlight the extent to which their activities cover all aspects of IoT security and the extent to which established standards, such as the ISO/IEC 27000 series, apply to the IoT.

3.1 Formal Standards Relevant to IoT Security

At present, the development of formal standards pertaining to IoT security is relatively slow moving. There are at least two reasons that explain this pace of development. First, formal standardisation processes are generally longer than market-driven ones, due to the highly institutionalised approval and review process. In addition, formal standards development in regional and international organisations is more politicised, due to the complex voting structure (e.g. national weighted voting in ETSI) or the competitive promotion of national standards for international adoption (e.g. ISO or ITU).

Second, the topology of the IoT ecosystem (i.e. edge, connectivity, services) as well as its large application area (e.g. consumer goods, critical infrastructure and essential services) challenge the current organisation of formal standards development activities. This can be observed through the development of formal standards in the International Organisation for Standardisation (ISO) [40–43] and the national and regional standardisation organisations [44] that have partnered to create oneM2M [45] (Figure 4).

In addition, the formal standards landscape is complicated by standardisation activities pertaining to specific IoT application areas, such as the development of security standards for smart grid systems in CEN/CENELEC (EU) [46] or NIST (US) [47].

Thus, although formal standardisation processes relevant to IoT security are advancing, it is difficult to say that a baseline for IoT security has so far been achieved in formal SDOs. As seen in the case of ISO (Figure 4), the IoT challenges the organisation of formal standardisation activity, and requires coordination and a more careful alignment between technical committees working on IoT architecture and interoperability,

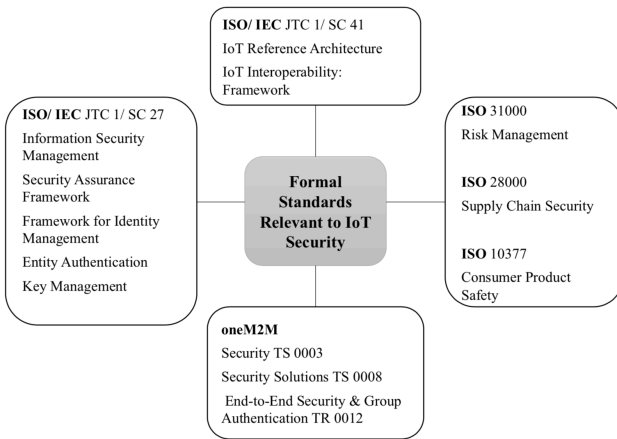


Fig. 4: Formal Published Standards Relevant to IoT Security

security, risk management, supply chain management and consumer product safety.

3.2 De Facto Standards Relevant to IoT Security

Several industry alliances and interest associations have responded to the gaps in formal standards development by proposing their own guidelines for securing the IoT. Increasingly, these guidelines are complemented by compliance testing procedures for members or interested parties. Some industry associations are also promoting their own certification labels and trust marks, as a way of showcasing compliance with the proposed guidelines. In addition, open certification marks are currently developed by not-for-profit organisations targeting consumers and start-up companies [48].

Table 1 provides a summary of the main industry and interest associations that have to this date developed IoT security-related guidelines [34–39], [49–56], compliance testing pro-

Industry Association & Guidelines	Compliance Testing	Certification
Open Web Application Security Project (OWASP) Principles of IoT Security IoT Security Guidance	IoT Framework Assessment IoT Testing Guides IoT Testing Methodology	N/A
Online Trust Alliance (OTA) IoT Security & Privacy Trust Framework	Online Trust Audit	Honour Rolls
Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT Future Proofing the Connected World	Cloud Control Matrix Consensus Assessments Initiative Questionnaire	CSA STAR self-assessment, 3 rd party, or continuous monitoring certification
Broadband Internet Technical Advisory Group (BITAG) Internet of Things Security and Privacy Recommendations	N/A	N/A
Open Connectivity Foundation (OCF) Security Specifications	OCF Testing and Certification Program	OCF Certification Mark
GSM Association (GSMA) IoT Security Guidelines for: - Endpoint Ecosystems - Network Operators - Service Ecosystem	IoT Security Assessment Checklist Self-Assessment Scheme	Once IoT Security Assessment is approved, product is listed on GSMA IoT website.
IoT Security Foundation (IoTSF) Connected Consumer Products Best Practice Guidelines Vulnerability Disclosure Best Practice Guidelines	IoT Security Compliance Framework	Best Practice User Mark
Industrial Internet Consortium (IIC) Industrial Internet Security Framework	Security Checklists for Verticals Maturity Models for Industrial Systems	N/A

Table 1: Market-Driven Guidelines, Testing and Certification Frameworks for IoT Security

cedures and certification marks [57–67] to signal their conformity with a responsible level of IoT security.

Table 1 shows that the *IoT security standards and best practice landscape has been predominantly shaped by the market* via transnational industry alliances and interest associations. A quick review of the guidelines, testing and certification schemes proposed by these associations reveals three main findings.

First, there is growing *convergence in de facto standardisation towards a set of core technical and organisational specifications* to ensure a responsible level of IoT security. This convergence has also been noted by cybersecurity agencies and standardisation bodies in the EU and the US [30, 32, 68], and includes:

Core Technical Specifications

- Identification, authentication, authorization
- Cryptography
- Security auditing
- Self-protection and component isolation
- Data integrity and minimisation

Core Organisational Specifications

- Risk and asset management
- Threat analysis and use case assessments
- Lifecycle and end-of-life support
- User awareness through clear policies and labelling

Second, the development of de facto guidelines and certification schemes increases the complexity of the current standards landscape for IoT security, especially for new entrants and small and medium size enterprises (SMEs) who have to navigate through the complex landscape of standards, guidelines and best practices currently available.

Participants of the ‘Secure by Default’ Workshop organised by PETRAS IoT (March 2017) echoed this, emphasising that the decision to select the most appropriate standards for their particular business is one of the main challenges faced by entities in the IoT ecosystem, especially at the manufacturing and service level.

In addition, the PETRAS IoT ‘Cybersecurity of the Internet of Things Standards Survey’ revealed an already mixed picture when it comes to the ease of implementing and deploying current standards for IoT security (Figure 5). This reality can explain, at least in part, why legislators and public agencies are increasingly preoccupied with setting a level playing field for IoT security.

Lastly, current IoT security best practices expose new interdependencies that challenge and will continue to challenge standardisation processes in the future. The list of market-driven

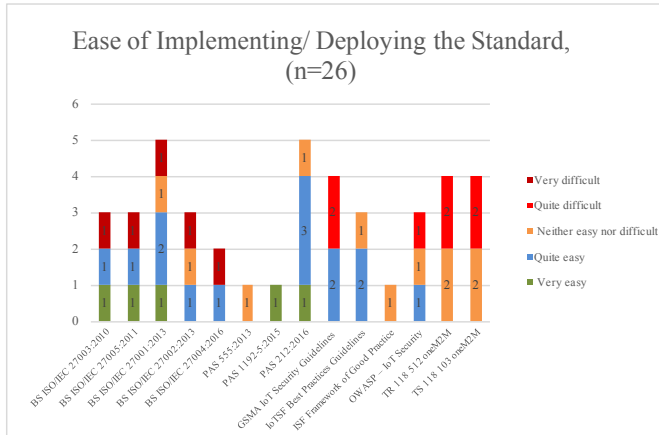


Fig. 5: Ease of Implementing and Deploying Standards Related to Cybersecurity of the IoT. Data shows responses to Question 13 of the ‘Cybersecurity of the Internet of Things Standards Survey’[9]: “How easy to implement/ deploy was the standard or standards?”.

guidelines in Table 1 uncovers new tensions in setting a unique baseline for IoT security across its multiple application areas and domains, most importantly the relationships between: a) cyber security, physical security and safety, and b) trust as consumer protection, service reliability and system resilience. For instance, a majority of the reviewed guidelines identify consumer trust as a fundamental aspect of IoT security governance. However, the proposed principles and practices that correspond to ensuring consumer trust vary considerably, ranging from lifecycle security controls and patching, to privacy and vulnerability disclosure policies, to safety impact assessments.

4 Conclusions

The current paper reviewed the main IoT security standards and guidelines that have been established by formal regional and international standardisation organisations, as well as by transnational industry associations and alliances to date. Drawing on desk-based research as well as survey and workshop data, the review uncovers the fragmented nature of the IoT standardisation landscape and some of the main challenges to IoT security standards development.

First, the analysis of both a) Policies, Regulatory Frameworks and High-Level Guidelines for IoT Security and b) Industry Codes of Practice, Technical Specifications and Certification Schemes showed the extent to which standardisation efforts are leading towards the *establishment of a baseline for IoT security* in some of the most developed IoT markets, with particular focus on the UK, EU and US.

Second, the paper highlighted that the IoT security standards landscape is dominated by *de facto standards* initiated by a diverse range of industry associations across the IoT ecosystem. The development of *de facto* guidelines and certifica-

tions schemes increases the complexity of the current standards landscape and reinforces fragmentation as well as the difficulty for new entrants and SMEs to identify the most suitable standards and guidelines currently available.

Third, the paper identified a number of key challenges for the current IoT security standards landscape, most notably: a) the difficulty of setting a baseline for IoT security across all IoT applications and domains, which adds complexity to defining specifications that clarify the relationship between data integrity — cyber and physical security — safety — resilience — trustworthiness; as well as b) the difficulties of monitoring the adoption and implementation of IoT security standards and best practices by market entities involved in the development, manufacturing and service provision of IoT.

The analysis of the evolution and current state of deployment of IoT security standards contributes to a better understanding of the need for a more aligned standardisation approach. Standards development organisations are encouraged to seek more extensive coordination across technical committee and have to a) fill the gap of developing formal security standards which take into account both device and end-to-end security, and are specific to the IoT; and b) articulate more clearly the extent to which their activities cover all aspects of IoT security and the extent to which their published standards, such as information security standards, apply to the IoT.

Additionally, the review affirmed that more research on the barriers to adoption and implementation of IoT security standards is needed. This will be pursued by the PETRAS IoT Research Hub in the course of a further analysis stage which involves semi-structured interviews with key standards development organisations, trade associations and UK regulatory bodies. This holistic assessment can feed into ongoing policy reviews and standardisation processes, by revealing the main opportunities and challenges to achieving a secure IoT.

Acknowledgements

The authors would like to express their appreciation to Robert Thompson (PETRAS IoT, UCL), Graca Carvalho (PETRAS IoT, UCL), Tim McGarr (BSI), Alberto Garcia Mogollon (BSI) and Idris Jahn (IoTUK) for their valuable contribution to the development and dissemination of the ‘Cybersecurity of the Internet of Things Survey’ and the coordination of the ‘IoT Secure by Default’ Workshop.

This research was supported by the UK Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1.

References

- [1] Cambridge Consultants, ‘Review of Latest Developments in the Internet of Things.pdf’, OFCOM, May 2017.
- [2] Gartner, ‘Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From

- 2016', 02-Jul-2017. [Online]. Available: <https://www.gartner.com/newsroom/id/3598917>. [Accessed: 08-Jan-2018].
- [3] Vodafone, 'Vodafone IoT Barometer 2017/2018'. Sep-2017.
- [4] Cisco, '2017 Midyear Cybersecurity Report', Jul. 2017.
- [5] Ovum, 'Ovum Viewpoints: IoT Opportunities in 2017 and Beyond', Jul. 2017.
- [6] C. Maple, 'Security and privacy in the internet of things', *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017.
- [7] D. M. Mendez, I. Papapanagiotou, and B. Yang, 'Internet of Things: Survey on Security and Privacy', *arXiv:1707.01879 [cs]*, Jul. 2017.
- [8] J. Granjal, E. Monteiro, and J. S. Silva, 'Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues', *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.
- [9] PETRAS IoT, BSI Group, and IoT UK, 'Cybersecurity of the Internet of Things Standards Survey, IoT Multi-disciplinary Standards Platform Project (IoTMSP)'. Mar-2017.
- [10] UK Government Office of Science, 'The Internet of Things: Making the Most of the Second Digital Revolution: A Report by the UK Government Chief Scientific Adviser', 2016.
- [11] ENISA, *Security Challenges and Best Practices in the IoT Environment, Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht. Public Hearing on Security Challenges and Best Practices in the IoT Environment*. 2017.
- [12] NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching, 'Communicating IoT Device Security Update Capability to Improve Transparency for Consumers'. 25-Apr-2017.
- [13] L. Tanczer, F. Yahya, I. Brass, M. Elsdén, J. Blackstock, and M. Carr, 'International Developments on the Security of the Internet of Things.', PETRAS IoT.
- [14] R. Baldwin, M. Cave, and M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Second Edition. Oxford, New York: Oxford University Press, 2011.
- [15] UK Department for Digital, Culture, Media and Sport, 'Cyber Security Regulation and Incentives Review', Dec. 2016.
- [16] UK National Cyber Security Centre (NCSC), 'Secure by Default Principles', May-2017. [Online]. Available: <https://www.ncsc.gov.uk/articles/secure-default>. [Accessed: 11-Jan-2018].
- [17] I. Brass, L. Tanczer, M. Carr, M. Elsdén, and J. Blackstock, 'IoT Security: A Review of the Regulatory and Standards Landscape. Presentation at the Royal Society (RS) Conference "Internet of Things: Opportunities and Threats"', 11-Mar-2017.
- [18] I. Brass, L. Tanczer, M. Carr, and J. Blackstock, 'Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things?', *CARR Risk and Regulation Magazine*, vol. 33, Aug. 2017.
- [19] L. Tanczer, I. Brass, M. Elsdén, M. Carr, and J. Blackstock, 'The United Kingdom's Emerging Internet of Things (IoT) Policy and Legislative Landscape', in *Rewired: Cybersecurity Governance*, Wiley, forthcoming.
- [20] UK Department for Transport, *The Key Principles of Cyber Security for Connected and Automated Vehicles*. 2017.
- [21] US Department for Homeland Security, *Strategic Principles for Securing the Internet of Things*. 2016.
- [22] US National Highway Traffic Safety Administration (NHTSA), *Federal Automated Vehicles Policy: Accelerating the Next Revolution In Roadway Safety*. 2016.
- [23] US Food and Drug Administration, *Content of Pre-market Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. 2014.
- [24] US Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. 2016.
- [25] US Senate, 'Internet of Things Cybersecurity Improvement Act'. Jul-2017.
- [26] European Commission, *COM(2017) 477 Final Proposal for a Regulation of The European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*. 2017.
- [27] US National Telecommunications and Information Administration (NTIA), 'Voluntary Framework for Enhancing Update Process Security', Oct. 2017.
- [28] US Federal Trade Commission (FTC), 'Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers" Communicating Upgradability

- and Improving Transparency Working Group Multistakeholder Process on Internet of Things Security Upgradability and Patching National Telecommunications & Information Administration'. Apr-2017.
- [29] NIST, 'Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Special Publication 800-160.'
- [30] ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructure', Nov. 2017.
- [31] NTIA, 'Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching'. [Online]. Available: <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security>. [Accessed: 11-Jan-2018].
- [32] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity, Draft 2', 12-May-2017. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf. [Accessed: 11-Jan-2018].
- [33] ENISA, 'Gaps in NIS standardisation: Recommendations for improving NIS in EU standardisation policy', Nov. 2016.
- [34] GSMA, 'IoT Security Guidelines Overview', Feb-2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-guidelines-overview-document/>.
- [35] GSMA, 'IoT Security Guidelines for Endpoint Ecosystems', Feb-2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/>.
- [36] GSMA, 'IoT Security Guidelines for Network Operators', Feb-2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/>.
- [37] GSMA, 'IoT Security Guidelines for Service Ecosystems', Feb-2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/>.
- [38] OWASP, 'Principles of IoT Security', 2016. [Online]. Available: https://www.owasp.org/index.php/Principles_of_IoT_Security. [Accessed: 15-Aug-2017].
- [39] OWASP, 'IoT Security Guidance', 2016. [Online]. Available: https://www.owasp.org/index.php/IoT_Security_Guidance. [Accessed: 15-Aug-2017].
- [40] ISO/ IEC, 'ISO/IEC JTC 1/SC 27 - IT Security techniques, Standards in Development'. [Online]. Available: <https://www.iso.org/committee/45306/x/catalogue/p/0/u/1/w/0/d/0>. [Accessed: 03-Jan-2018].
- [41] ISO/ IEC, 'ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies - Standards in Development'. [Online]. Available: <https://www.iso.org/committee/6483279/x/catalogue/p/0/u/1/w/0/d/0>. [Accessed: 03-Jan-2018].
- [42] ISO, 'ISO 31000 Risk management'. [Online]. Available: <https://www.iso.org/iso-31000-risk-management.html>. [Accessed: 14-Jan-2018].
- [43] ISO, 'ISO 28000:2007 - Specification for security management systems for the supply chain'. [Online]. Available: <https://www.iso.org/standard/44641.html>. [Accessed: 14-Jan-2018].
- [44] OneM2M, 'oneM2M - Partners'. [Online]. Available: <http://www.onem2m.org/about-onem2m/partners>. [Accessed: 14-Jan-2018].
- [45] OneM2M, 'oneM2M - Published Specifications'. [Online]. Available: <http://www.onem2m.org/technical/published-documents>. [Accessed: 14-Jan-2018].
- [46] CEN-CENELEC, 'Smart grids'. [Online]. Available: <https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>. [Accessed: 13-Jan-2018].
- [47] NIST, 'Guidelines for Smart Grid Cybersecurity', 2014. [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>. [Accessed: 14-Jan-2018].
- [48] The IoT Mark, 'The 30 principles', 18-Oct-2017. [Online]. Available: <https://iotmark.wordpress.com/principles/>. [Accessed: 30-Oct-2017].
- [49] OTA, 'IoT Security & Privacy Trust Framework V2.5', Jun-2017. [Online]. Available: https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf.
- [50] Cloud Security Alliance, 'New Security Guidance for Early Adopters of the IoT', 2015. [Online]. Available: <https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/>.
- [51] Cloud Security Alliance, 'Future Proofing the Connected World: 12 Steps to Developing Secure IoT

- Products', 2016. [Online]. Available: <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf>. [Accessed: 15-Aug-2017].
- [52] BITAG, 'IoT Security and Privacy Recommendations', 2016. [Online]. Available: [https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf). [Accessed: 16-Aug-2017].
- [53] OCF, 'Security Specifications', 2017. [Online]. Available: https://openconnectivity.org/draftspecs/OCF_Security_Specification_v1.0.0.pdf.
- [54] IoT SF, 'Connected Consumer Products: Best Practice Guidelines', 2016. [Online]. Available: <https://iotsecurityfoundation.org/best-practice-guidelines/>.
- [55] IoT SF, 'Vulnerability Disclosure: Best Practice Guidelines', 2016. [Online]. Available: <https://iotsecurityfoundation.org/best-practice-guidelines/>.
- [56] IIC, 'Industrial Internet Security Framework'. [Online]. Available: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf.
- [57] OWASP, 'IoT Framework Assessment', 2016. [Online]. Available: https://www.owasp.org/index.php/IoT_Framework_Assessment. [Accessed: 15-Aug-2017].
- [58] OWASP, 'IoT Testing Guides', 2014. [Online]. Available: https://www.owasp.org/index.php/IoT_Testing_Guides. [Accessed: 15-Aug-2017].
- [59] OWASP, 'IoT Testing Methodology', 2017. [Online]. Available: <https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf>. [Accessed: 15-Aug-2017].
- [60] OTA, '2017 Online Trust Audit and Honour Rolls', Jul-2017. [Online]. Available: <https://otalliance.org/system/files/files/initiative/documents/2017trustaudit.pdf>.
- [61] CSA, 'Security, Trust & Assurance Registry (STAR)'. [Online]. Available: <https://cloudsecurityalliance.org/star/>. [Accessed: 18-Aug-2017].
- [62] OCF, 'OCF Security FAQ'. [Online]. Available: <https://openconnectivity.org/foundation/faq/ocf-security-faq>. [Accessed: 16-Aug-2017].
- [63] OCF, 'OCF Certification', *Open Connectivity Foundation (OCF)*. [Online]. Available: <https://openconnectivity.org/certification>. [Accessed: 18-Aug-2017].
- [64] GSMA, 'IoT Security Assessment', 2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-assessment/>.
- [65] GSMA, 'IoT Security Checklist', 2016. [Online]. Available: <https://www.gsma.com/iot/iot-security-assessment/>.
- [66] IoT SF, 'IoT Security Compliance Framework', 2016. [Online]. Available: <https://iotsecurityfoundation.org/best-practice-guidelines/>.
- [67] IC, 'Frequently Asked Questions about IISF | How can you demonstrate the IISF techniques?' [Online]. Available: <http://www.iiconsortium.org/IISF-faq.htm>. [Accessed: 14-Jan-2018].
- [68] IEEE, 'Internet of Things (IoT) Security Best Practices', Feb-2017. [Online]. Available: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf. [Accessed: 03-Jan-2018].